Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б.Жильцов
« 14 » 09 2018 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ»

для студентів

спеціальності	111 Математика
освітнього рівня	другого (магістерського)
освітньої програми	111.00.02 Математичне моделювання

Київ – 2018

Розробник:

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладач:

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від 13.09.2018 р. № 6

Завідувач кафедри _____ (підпис) В.Л. Бурячок

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 111.00.02 Математичне моделювання)

___.___. 20___ р.

Керівник освітньої програми _____ (підпис) В.В. Прошкін

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ (підпис) І.Ю. Мельник

Пролонговано:

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	6 / 180	
Курс	6	
Семестр	11	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	6	
Обсяг годин, в тому числі:	180	
Аудиторні	48	
Модульний контроль	12	
Семестровий контроль		
Самостійна робота	120	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Математичні основи криптографії» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчальних планів спеціальності 111 Математика, освітньої програми 111.00.02 Математичне моделювання.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Математичні основи криптографії» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Математичні основи криптографії» складається з 3-х змістових модулів: 1.Основні поняття безпеки інформації. Математичні основи; 2.Асиметричні криптосистеми на базі кілець; 3.Асиметричні криптосистеми на базі полів. Обсяг дисципліни – 180 год (6 кредитів).

Метою викладання навчальної дисципліни «Математичні основи криптографії» є отримання компетентностей в області криптографічного захисту інформації у комп’ютерних мережах .

Завдання:

- надання студентам теоретичних знань про задачі та особливості криптографічного захисту інформації у комп’ютерних мережах .
- формування у студентів категоріальних понять з основ математики асиметричної криптографії;
- формування у студентів умінь обчислювати параметри цифрового підпису і розподілу ключів на основі відомих протоколів;
- стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів розвитку у сфері захисту інформації.

У результаті вивчення навчальної дисципліни формуються

загальні компетентності:

- ***компетентності у сфері навчання:***

- здатність до організації самостійної навчальної, практичної та науково-дослідної діяльності;

- ***компетентності у сфері застосування знань в практичних ситуаціях***
  - вміння застосовувати здобуті теоретико-концептуальні професійні знання у процесі практичної, викладацької та науково-дослідної роботи;

фахові компетентності:

- ***компетентності у сфері теоретичних основ криптографічного захисту інформації:***
  - глибокі знання та розуміння змісту і задач асиметричної криптографії з використанням ІКТ;
  - уміння обчислювати параметри цифрового підпису і розподілу ключів на основі відомих протоколів;
  - компетентності у сфері діагностико-аналітичної і консультативної діяльності для реалізації ІТ рішень;
- **компетентності у сфері науково-дослідної діяльності:**
  - уміння вивчати і систематизувати досягнення вітчизняних і зарубіжних досліджень у галузі інформаційно-комунікаційних технологій, суміжних галузей знань;
  - вивчати, узагальнювати й упроваджувати на практиці вітчизняний і зарубіжний досвід управління інформаційними технологіями і системами.
- **компетентності у сфері вмінь працювати в групі:**
  - здатність використовувати навички взаємодії в роботі, компетентності у сфері навичок міжособистісного спілкування
  - здатність до продуктивного використання комунікації як складової професійної діяльності.

3. Результати навчання за дисципліною

При вивченні курсу «Математичні основи криптографії» студенти повинні

знати:

- про джерела і способи дії загроз на об’єкти інформаційної безпеки установ;
- про правові і нормативні акти, які визначають систему захисту інформації в державі;
- про основні методи, технологію, принципи і правила побудови захисту електронних обчислювальних машин, у тому числі персональних комп’ютерів, їх елементів і об’єктів комп’ютерних мереж;
- про алгоритми створення сучасних програм, алгоритми шифрування та застосування стандартного програмного забезпечення захисту;
- про методи та технології захисту операційних систем, текстових редакторів, табличних процесорів, системи управління базами даних в локальних, корпоративних та глобальних комп’ютерних мережах.

уміти:

- працювати з концептуальними моделями розробки, розподілу, обробки, використання та зберігання конфіденціальних документів;
- визначати системи й методи захищеності носіїв інформації;
- створювати засобами стандартного програмного забезпечення елементи захисту інформації.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1 Основні поняття безпеки інформації. Математичні основи							
Тема 1.Основні поняття безпеки інформації	12	2					10
Тема 2.Математичні основи . Теорія чисел. Модульна арифметика. Кінцеві групи, кільця і поля	14	2		2			10
Тема 3.Мультиплікативні групи полів і кілець	16	2		4			10
Тема 4.Розподіл ключів за схемою Діффі-Хелмана	14	2		2			10
Модульний контроль	4						
Разом	60	8		8			40
Змістовий модуль 2. Асиметричні криптосистеми на базі кілець							
Тема 5. Криптосистема RSA	16	2		4			10
Тема 6. Ключові пари RSA	14	2		2			10
Тема 7. Цифровий підпис RSA	14	2		2			10
Тема 8. Безпека RSA	12	2					10
Модульний контроль	4						
Разом	60	8		8			40
Змістовий модуль 3. Асиметричні криптосистеми на базі полів							
Тема 9. Криптосистема Ель-Гамаля	16	2		4			10
Тема 10. Цифровий підпис DSA	14	2		2			10
Тема 11. Цифровий підпис Р34-310	14	2		2			10
Тема 12. Стандарти цифрового підпису	12	2					10
Модульний контроль	4						
Разом	60	8		8			40
Усього	180	24		24	8		120

5. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття безпеки інформації. Математичні основи

Тема 1. Вступ. Основні поняття безпеки інформації

Основні загрози інформаційній безпеці. Категорії безпеки інформації в комп'ютерних мережах та інформаційних системах. “Помаранчева книга” США. Методи захисту інформації. Задачи технічного і криптографічного захисту інформації. Моделі симетричної і асиметричної криптосистем

Тема 2. Математичні основи . Теорія чисел. Модульна арифметика. Кінцеві групи, кільця і поля

Модульна арифметика. Визначення групи, кільця і поля, приклади. Кінцеві групи. і кільця. Циклічні групи. Прості поля Галуа. Мультиплікативні порядки елементів. Функція Ейлера

Тема 3. Мультиплікативні групи полів і кілець

Мультиплікативна група простого поля Галуа, порядок групи, властивості. Порядок елемента групи. Підгрупи. Кількість елементів однакового порядку. Мультиплікативна група кільця за не простим модулем. Нециклічні групи та їх підгрупи. Порядок елемента групи кільця. Узагальнена функція Ейлера.

Тема 4. Розподіл ключів за схемою Діффі-Хелмана

Визначення однобічної функції та її приклади. Функція експоненціювання у кінцевому полі. Проблема дискретного логарифму. Розподіл ключів за схемою Діффі-Хелмана

Змістовий модуль 2. Асиметричні криптосистеми на базі кілець

Тема 5. Криптосистема RSA

Побудова мультиплікативної групи кільця по модулю N = PQ, визначення порядку МГ кільця і максимального порядку елементів МГ. Функція Ейлера і узагальнена функція Ейлера. Знаходження зворотних елементів МГ. Структура МГ кільця. Функції шифрування-дешифрування RSA. Визначення ключової пари RSA. Секретні і відкриті ключі.

Тема 6. Ключові пари RSA

Простір ключів RSA та його розмір. Розрахунок максимального порядку ключа. Методи розрахунку ключових пар. Паразитні ключі та ключі-близнюки.

Тема 7. Цифровий підпис RSA Властивості хеш-функції повідомлення. Цифровий підпис RSA Безпека RSA. Складність факторизації модуля N = PQ.

Тема 8. Безпека RSA

Проблема факторизації великих чисел. Субекспоненційна оцінка складності розкладання великого числа на множники. Приклади. Вимоги до модуля згідно сучасних стандартів

Змістовий модуль 3. Асиметричні криптосистеми на базі полів

Тема 9. Криптосистема Ель-Гамаля

Загальносистемні параметри RSA в криптосистемі Ель-Гамаля. Вимоги до параметрів. Напрямкове шифрування Ель-Гамаля. Цифровий підпис Ель-Гамаля

Тема 10. Цифровий підпис DSA

Загальносистемні параметри КС. Формування ЦП згідно з DSA. Ключове рівняння. Формування і перевірка цифрового підпису DSA Стандарти цифрового підпису. Цифровий підпис ГОСТ Р34.310.

Тема 11. Цифровий підпис Р34-310

Історична довідка. Формування і перевірка цифрового підпису згідно стандарту **Р34-310.** Переваги та недоліки стандарту

Тема 12. Стандарти цифрового підпису

Огляд та аналіз сучасних національних і міжнародних стандартів цифрового підпису і розподілу ключів. Криптосистеми на еліптичних кривих. Пост квантова криптографія

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.

- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	4	4	4	4
Відвідування семінарських занять							
Відвідування практичних занять	1	4	4	4	4	4	4
Відвідування лабораторних занять							
Робота на семінарському занятті							
Робота на практичному занятті	10	4	40	4	40	4	40
Лабораторна робота (в тому числі допуск, виконання, захист)							
Виконання завдань для самостійної роботи	5	2	10	2	10	2	10
Виконання модульної роботи	25	1	25	1	25	1	25
Виконання ІНДЗ	30						
Разом		-	83	-	83	-	83
Максимальна кількість балів: 249							
Розрахунок коефіцієнта: 249/100=2,49							

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної

дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Основні поняття безпеки інформації. Математичні основи		40	10
1	Тема 1.Основні поняття безпеки інформації Тема 2.Математичні основи . Теорія чисел. Модульна арифметика. Кінцеві групи, кільця і поля опрацювання фахових видань. Тема 3.Мультиплікативні групи полів і кілець Тема 4.Розподіл ключів за схемою Діффі-Хелмана	40	10
Змістовий модуль 2. Асиметричні криптосистеми на базі кілець		40	10
2	Тема 5. Криптосистема RSA Тема 6. Ключові пари RSA. . Тема 7. Цифровий підпис RSA Тема 8. Безпека RSA	40	10
Змістовий модуль 3. Асиметричні криптосистеми на базі полів		40	10
3	Тема 9.. Криптосистема Ель-Гамаля Тема 10.. Цифровий підпис DSA Тема 11.. Цифровий підпис Р34-310 Тема 12.. Стандарти цифрового підпису	40	10
	Разом	120	30

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	4 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	4 бали
3	Дотримання вимог щодо технічного оформлення	2 бал
	Разом	10 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Питання для самоконтролю

1. Загрози безпеки комп'ютерних мереж і систем.
2. Методи захисту комп'ютерних мереж і систем.
3. Методи захисту від несанкціонованого доступу
4. Задачі технічного захисту інформації
5. Задачі криптографічного захисту інформації

6. Блок-схема симетричної криптосистеми
7. Блок-схема асиметричної криптосистеми
8. Модульна арифметика.
9. Кінцеві структури: групи.
10. Зворотні елементи адитивної групи.
11. Зворотні елементи мультиплікативної групи.
12. Порядок групи і порядок елемента групи.
13. Підгрупи.
14. Генератори групи і підгрупи.
15. Кількість генераторів груп і підгруп.
16. Циклічні і нециклічні групи
17. Кінцеві структури: кільця.
18. Мультиплікативна група кільця.
19. Кінцеві структури: поля.
20. Функція Ейлера.
21. Узагальнена функція Ейлера, що вона визначає.
22. Визначення НОД (a,b) за допомогою алгоритму Евкліда.
23. Мультиплікативна група кільця за модулем N = PQ.
24. Структура МГ кільця за модулем N = PQ.
25. Розподіл ключів по схемі Діффі-Гелмана (над кінцевим полем). Неінтерактивний протокол.
26. Розподіл ключів по схемі Діффі-Гелмана (над кінцевим полем). Інтерактивний протокол.
27. Криптосистема RSA. Функції шифрування-дешифрування.
28. Напрямкове шифрування RSA.
29. Цифровий підпис RSA.
30. Криптосистема Ель-Гамаля. Напрямкове шифрування.
31. Цифровий підпис Ель-Гамаля.
32. Цифровий підпис DSA
33. Цифровий підпис ГОСТ Р34.310
34. . Безпека асиметричних КС.
35. Безпека симетричних КС.

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов’язковим повторним вивченням курсу -

		досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична карта дисципліни

Разом:180 год., лекції – 24 год., практичні заняття – 24 год., модульний контроль – 12 год., самостійна робота – 120 год.

Модулі (назви, бали)	**Змістовий модуль 1** (83 бали)				**Змістовий модуль 2** (83 бали)				**Змістовий модуль 3** (83 бали)			
Лекції (теми, бали)	1.Задачі технічного і криптографічного захисту інформації (1бал)	2. Теорія чисел та алгебраїчні структури (1бал)	3. Властивості циклічних та нециклічних груп (1бал)	4. Розподіл ключів за схемою Діфі-Гелмана (1бал)	5. Криптосистема RSA. Функція шифрування RSA (1бал)	6. Секретний і відкритий ключі RSA . Узагальнена функція Ейлера для їх розрахунку. (1бал)	7. Цифровий підпис RSA. Вимоги до хеш-функції .(1бал)	8. Безпека RSA. Проблема факторизації великих чисел (1бал)	9. риптосистема Ель-Гамаля. Шифрування і цифровий підпис (1бал)	10. Цифровий підпис згідно DSA. (1бал)	11. Цифровий підпис згідно ГОСТ Р34.310. (1бал)	12. Стандарти асиметричної криптографії. (1бал)
Практичні заняття (теми, бали)	1.Елементи теорії чисел. Задачі (11балів)	2. Побудова адитивної групи за модулем n (11балів)	3.Побудова мультиплікативної група за модулем р (11балів) (11балів)	4. Побудова мультиплікативної група за модулем n (11балів (11балів)	5. Функція шифрування RSA (11балів)	6. Розрахунок ключової пари (11балів)	7.Цифровий підпис RSA (11балів)	8. Безпека RSA (11балів)	9. Шифрування за схемою Ель-Гамаля (11балів)	10. Цифровий підпис за схемою Ель-Гамаля (11балів)	11. Цифровий підпис DSA (11балів)	12. Цифровий підпис ГОСТ Р34-310 (11балів)
Самост. робота	Самостійна робота (10 балів)				Самостійна робота (10 балів)				Самостійна робота (10 балів)			
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)				Модульна контрольна робота 2 (25 балів)				Модульна контрольна робота 3 (25 балів)			
Підсумковий контроль (вид, бали)	залік											

8. Рекомендовані джерела

Основна

1. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых.-К.: Изд. «Политехника», 2004. – 224с.

2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328с.

3. Задірака В.К., Олексюк О.С.,.Недашковський М.О. Методи захисту фінансової інформації. Навчальний посібник. К.: Вища школа, 2000. – 460 с

4. Домарев В.В. Защита информации и безопасность компьютерных систем. - К.: Издательство «Диасофт», 1999. – 480с.

5. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.:КУДИЦ-ОБРАЗ, 2001 – 368с.

9. Інформаційні ресурси

1. Web сайт: www.Wikipedia.com

2. Продуктb Google [Електронний ресурс] // – Режим дост.: http://www.google.com.ua/intl/ru/about/products/ – Заголовок з екрана

3. http://itosvita.ucoz.ua/

4. Шевелева В. С. Web-квесты в процессе обучения школьников / В. С. Шевелева. – Режим доступа : http://www.openclass.ru/node/20147

5. http://rutube.ru/video/fdc52dfda2b5724843aa03438d2cb26d/

6. http://www.edutainme.ru/

7. https://sites.google.com/site/intelworksheets/0modul

8. http://elibrary.kubg.edu.ua/1548/7/Kocharayn_NDLIO.pdf